PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-045212
(43)Date of publication of application : 16.02.1999

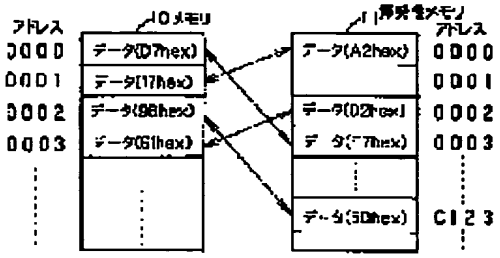
(51)Int.Cl. G06F 12/14

(21)Application number : 09-217025
(22)Date of filing : 29.07.1997

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : NARASHIMA TAKAAKI

(54) OPPOSING METHOD AGAINST DECIPHERING ATTACK REGARDING SECRET INFORMATION

(57)Abstract:
PROBLEM TO BE SOLVED: To oppose an attack for deciphering secret information by replacing and storing the secret information in a different place by electronic devices each time it is written to a volatile memory.
SOLUTION: Data on the address 0000 of secret information before conversion in a memory 10 are D7hex and when the secret information is stored for the first time according to a storage converting rule, it is stored in address 0003 of the volatile memory 11 by conversion to F7hex. For second storage, it is stored in address 0003 of the volatile memory 11 by conversion to code data other than F7hex. Similarly, data on the address 0001 are 17hex, first storage in the address 0003 of the volatile memory 11 is performed by conversion to A2hex, and data on the address 0002 are 9Bhex; and first storage in address C123 of the volatile memory 11 is performed by conversion to 5Dhex. Thus, the secret information is stored in different places by electronic devices each time it is stored in the memory.



LEGAL STATUS

[Date of request for examination] 27.06.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－45212

(43)公開日　平成11年(1999)２月16日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ ３２０Ｄ

審査請求　未請求　請求項の数３　ＦＤ　（全５頁）

(21)出願番号　特願平9－217025

(22)出願日　平成９年(1997)７月29日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　楢島　高明
神奈川県横浜市港北区網島東四丁目３番１号　松下通信工業株式会社内

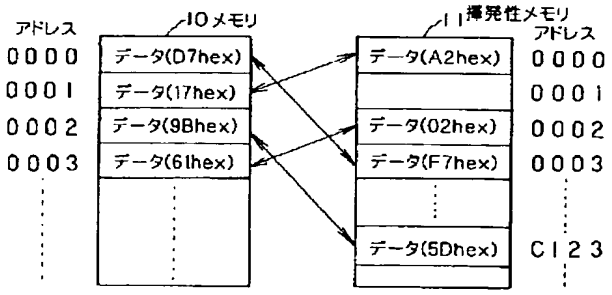
(74)代理人　弁理士　青木　輝夫

(54)【発明の名称】　秘密情報の解読攻撃対抗方法

(57)【要約】

【課題】　揮発性メモリに秘密情報を書き込む場合に該秘密情報の内容及び格納位置を変換することにより、秘密情報の解読の攻撃に対抗する。

【解決手段】　変換後の秘密情報を格納する揮発性メモリ１１を有する秘密情報の解読攻撃対抗方法において、書き込み時に情報を任意に変換する手段を具備し、この変換手段により秘密情報を電子機器毎及び揮発性メモリに書き込む毎に異なる場所に変換して格納する。



1

【特許請求の範囲】

【請求項１】　秘密情報を保持する揮発性メモリに対して、書き込み情報を任意に変換する手段を具備し、前記変換手段により秘密情報を電子機器毎及び揮発性メモリに書き込む毎に異なる場所に変換して格納することを特徴とする秘密情報の解読攻撃対抗方法。

【請求項２】　変換手段は、アドレス信号線及びデータ信号線の情報を任意に変換して各信号線の入れ替えを行うスイッチで構成され、該スイッチにより前記アドレス信号線及びデータ信号線任意に入れ替えられることを特徴とする請求項１記載の秘密情報の解読攻撃対抗方法。

【請求項３】　変換手段は、アドレス信号線及びデータ信号線の情報を任意に変換して各信号線の入れ替えるための情報が書き込まれる変換用メモリで構成され、該変換用メモリの情報により非線形に秘密情報が格納させることを特徴とする請求項１記載の秘密情報の解読攻撃対抗方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、筐体に収納された電子機器のメモリに保持されている秘密情報を解読しようとする攻撃に対抗する方法に関するものである。

【０００２】

【従来の技術】従来から秘密情報を保持した電子機器には、電子機器の筐体を分解し保持されている秘密情報をメモリから容易に読み出され解読されないようにする種々の方法が施されている。例えば、電子機器内部の揮発性メモリに格納された秘密情報を解読しようとする攻撃に対抗（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｔ）する方法として、メモリを容器に封入し外部からの攻撃を検知する手段を具備し、攻撃を受けるとメモリ内部の秘密情報を消去する方法が特開平２－４４４４７号公報等で知られている。

【０００３】

【発明が解決しようとする課題】しかしながら、上記のような従来の攻撃を検知してメモリ内部の秘密情報を消去する方法では、その消去する構造が解明されてしまうとバックアップされた揮発性メモリの秘密情報を消去せずに読み取ることが可能になる。例えば、複数の読み取られた情報の内容比較や情報が収納されている位置関係から解読する条件を与えるという問題がある。

【０００４】本発明は、上記のような問題を解決するものであり、揮発性メモリに秘密情報を書き込む場合に該秘密情報の内容及び格納位置を変換することにより、秘密情報の解読の攻撃に対抗できるようにした秘密情報の解読攻撃対抗方法を提供することを目的とする。

【０００５】

【課題を解決するための手段】上記課題を解決するために本発明は、秘密情報を保持する揮発性メモリに対して、書き込み情報を任意に変換する手段を具備し、前記

2

変換手段により秘密情報を電子機器毎及び揮発性メモリに書き込む毎に異なる場所に変換して格納することを特徴とする。

【０００６】本発明によれば、秘密情報の解読の攻撃に対抗できる。

【０００７】

【発明の実施の形態】本発明の請求項１に記載の発明は、秘密情報を保持する揮発性メモリに対して、書き込み情報を任意に変換する手段を具備し、前記変換手段により秘密情報を電子機器毎及び揮発性メモリに書き込む毎に異なる場所に変換して格納するものであり、揮発性メモリに書き込まれた秘密情報の位置が不特定となることにより、複数の読み出された秘密情報から解読の手がかりとなる情報を与えにくくすることができるという作用を有する。

【０００８】請求項２に記載の発明は、変換手段が、アドレス信号線及びデータ信号線の情報を任意に変換して各信号線の入れ替えを行うスイッチで構成され、該スイッチにより前記アドレス信号線及びデータ信号線任意に入れ替えられるものであり、アドレス及びデータの信号線数に対応した任意のアドレス順とデータのビット位置を入れ替えてアクセスすることができ、同じ秘密情報を各装置に書き込んでもメモリ上の情報は信号線の組み合わせ数まで装置単位で異なるようにすることができるという作用を有する。

【０００９】請求項３に記載の発明は、変換手段が、アドレス信号線及びデータ信号線の情報を任意に変換して各信号線の入れ替えるための情報が書き込まれる変換用メモリで構成され、該変換用メモリの情報により非線形に秘密情報が格納させるものであり、揮発性メモリに対して非線形の空間に秘密情報を格納することができ、かつ信号線の組み合わせ以上に変換して揮発性メモリをアクセスすることができるという作用を有する。

【００１０】以下、本発明の実施の形態について、図１～図５を用いて説明する。

【００１１】（実施の形態１）図１は、本発明の実施の形態１における秘密情報の解読攻撃対抗方法により秘密情報を揮発性メモリに任意の場所に情報を変換して格納する場合の原理説明図である。図１において、１０は変換される以前の秘密情報の格納状態を表したメモリであり、１１は電子機器毎及びメモリに書き込む毎に異なる格納変換法則に基づいて秘密情報を格納した後の状態を表す揮発性メモリである。

【００１２】この構成において、メモリ１０における変換以前の秘密情報のアドレス０００００番地のデータはＤ７ｈｅｘであり、この秘密情報の格納変換法則に基づく１回目の格納は、揮発性メモリ１１のアドレス０００３番地にＦ７ｈｅｘと変換されて格納される。また、２回目の格納は、揮発性メモリ１１のアドレス０００３番地にＦ７ｈｅｘ以外のコードデータに変換して格納され

る。

【００１３】以下同様にして、メモリ１０における変換以前の秘密情報のアドレス０００１番地のデータは１７ｈｅｘであり、この秘密情報の格納変換法則に基づく１回目の格納は、揮発性メモリ１１のアドレス０００３番地にＡ２ｈｅｘと変換されて格納され、また、メモリ１０における変換以前の秘密情報のアドレス０００２番地のデータは９Ｂｈｅｘであり、この秘密情報の格納変換法則に基づく１回目の格納は、揮発性メモリ１１のアドレスＣ１２３番地に５Ｄｈｅｘと変換されて格納される。同様にして、２回目の格納は、上記アドレス番地に上記以外のコードデータに変換して格納されることになる。また、揮発性メモリ１１に変換されて格納されている秘密情報を読み出す時は、格納時と逆の変換を行うことによりメモリ１０に示す変換以前の秘密情報に戻すことができる。

【００１４】このように電子機器毎及びメモリに書き込む毎に異なる場所に格納変換法則に基づき秘密情報を情報変換して揮発性メモリに格納するため、この揮発性メモリに格納された秘密情報を複数に亘り読み出して比較したとしても、解読するための特徴を解り難くすることが可能になる。

【００１５】（実施の形態２）図２～図４により本発明の実施の形態２について説明する。図２は実施の形態１の方法を、揮発性メモリとマイクロプロセッサ間を接続するアドレスバスとデータバスに変換回路を設けることで実現するようにしたブロック図であり、図３は変換回路を切替スイッチにより構成した場合のブロック図であり、図４は切替スイッチの構成図である。

【００１６】図２において、１２はマイクロプロセッサ（ＭＰＵ）、１３はマイクロプロセッサ１２の制御下で電子機器の外部から転送されてきた秘密情報を電子機器毎及びメモリに書き込む毎に異なる場所に格納変換法則に基づき変換する変換回路、１４は変換回路１３で変換された秘密情報を格納する揮発性メモリである。マイクロプロセッサ１２と変換回路１３間はアドレスバス１５とデータバス１６により接続され、変換回路１３と揮発性メモリ１４間はアドレスバス１７とデータバ１８により接続されている。

【００１７】図３において、変換回路１３は、マイクロプロセッサ１２のアドレス端子Ａ０～Ａｎ及びデータ端子Ｄ０～Ｄｍに対応する数の１：ｎのセレクトタイプのアドレス用切替スイッチＳＷＡ０、ＳＷＡ１・・・及び１：ｍのセレクトタイプのデータ用切替スイッチＳＷＤ０、ＳＷＤ１・・・から構成され、各アドレス用切替スイッチＳＷＡ０、ＳＷＡ１・・・の１入出力端はマイクロプロセッサ１２のアドレスＡ０～Ａｎのアドレス信号線に接続され、さらに、各アドレス用切替スイッチＳＷＡ０、ＳＷＡ１・・・のｎ入出力端の同じ信号線は揮発性メモリ１４のアドレスＡ０～Ａｎのアドレス信号線に並列に接続されている。また、データ用切替スイッチＳＷＤ０、ＳＷＤ１・・・の１入出力端はマイクロプロセッサ１２のデータＤ０～Ｄｍのデータ信号線に接続され、さらに、各データ用切替スイッチＳＷＤ０、ＳＷＤ１・・・のｎ入出力端の同じ信号線は揮発性メモリ１４のデータＤ０～Ｄｍのデータ信号線に並列に接続されている。

【００１８】図４はアドレス用及びデータ用切替スイッチの構成を示すもので、１：ｎまたは１：ｍのセレクトタイプのスイッチから構成され、この切替スイッチはマイクロプロセッサ１２からの制御信号ＳＷＳＥＬｘｘにより切替部ＳＷｘｘをｎまたはｍの入出力Ｂ、Ｃ、Ｄ・・・に切り替えることで、入出力Ａをｎまたはｍの入出力Ｂ、Ｃ、Ｄ・・・に切り替えるようになっている。

【００１９】上記の構成において、各切替スイッチの入出力Ｂ以降は同じ信号線同志で接続され、また、各切替スイッチはマイクロプロセッサ１２からの制御信号によりアドレスバス単位及びデータバス単位で同じ信号線が選択されるように制御されるから、例えば、切替スイッチＳＷＡ０入出力Ａは、マイクロプロセッサ１２のアドレスＡ０に接続され、切替スイッチＳＷＡ０の入出力Ｂ以降は揮発性メモリ１４のアドレスＡ０～Ａｎに接続される。そして、マイクロプロセッサ１２からの制御信号ＳＷＳＥＬｘｘにより、揮発性メモリ１４のアドレスＡ１が選択されているとすれば、切替スイッチＳＷＡ０以外の切替スイッチは揮発性メモリ１４のアドレスＡ１以外のアドレスが選択されることになる。また、データの場合もアドレスの場合と同様にして変換できる。

【００２０】従って、このような本実施の形態２によれば、マイクロプロセッサ１２のソフトウエアからは、同一のメモリ空間に見え、しかも不連続な任意のアドレス空間にデータを格納でき、かつ格納されたデータのビット位置の変えることができるから、同じ秘密情報を各電子機器に書き込んでもメモリ上の情報は信号線の組み合わせ数まで装置単位で異なるようすることができる。

【００２１】（実施の形態３）図５により本発明の実施の形態３について説明する。図５は変換回路１３に変換メモリを使用した場合の構成を示すブロック図である。

【００２２】図５において、変換回路１３は、アドレスを変換するための情報を書き込んだアドレス変換用メモリ１３１、データを書き込む時に変換するための情報を書き込んだデータ書き込み変換用メモリ１３２、データを読み込む時に変換するための情報を書き込んだデータ読み込み変換用メモリ１３３、及びデータを書き込む時とデータを読み込む時にデータバスを切り替えることによりデータ書き込み変換用メモリ１３２またはデータ読み込み変換用メモリ１３３を選択するデータバス切替器１３４、１３５を備える。

【００２３】上記の構成において、揮発性メモリ１４をアクセスするマイクロプロセッサ１２のアドレスはアド

5

レス変換用メモリ１３１により変換され、この変換されたアドレスを揮発性メモリ１４に出力することにより、揮発性メモリ１４は図１に示すように非線形にアクセスされることになる。また、秘密情報の書き込み時は、マイクロプロセッサ１２のデータバスがデータバス切替器１３４によりデータ書き込み変換用メモリ１３２のアドレスバスに接続され、かつデータ書き込み変換用メモリ１３２のデータバスはデータバス切替器１３５により揮発性メモリ１４のデータバスに接続される。また、秘密情報の読み込み時は、揮発性メモリ１４のデータバスがデータバス切替器１３５によりデータ読み込み変換用メモリ１３３のアドレスバスに接続され、かつデータ読み込み変換用メモリ１３３のデータバスはデータバス切替器１３４によりマイクロプロセッサ１２のデータバスに接続される。

【００２４】従って、それぞれの変換用メモリ１３１、１３２、１３３に非線形になるような情報を書き込んでおくことにより、アドレス及びデータの信号線の組み合わせ以上に変換してアクセスすることができる。

【００２５】

【発明の効果】以上のように本発明によれば、揮発性メモリに書き込まれた秘密情報の位置が不特定となることにより、複数の読み出された秘密情報から解読の手がかりとなる情報を与えにくくすることができる。

【００２６】また本発明によれば、アドレス信号線及びデータ信号線の情報を任意に変換する手段をスイッチで構成することにより、アドレス及びデータの信号線数に対応した任意のアドレス順とデータのビット位置を入れ替えてアクセスすることができ、このため、同じ秘密情報を各装置に書き込んでもメモリ上の情報は信号線の組み合わせ数まで装置単位で異なるようにすることができる。

【００２７】また本発明によれば、アドレス信号線及び

6

データ信号線の情報を任意に変換するための情報を書き込んだ変換用メモリの情報により、揮発性メモリに対して非線形の空間に秘密情報を格納することができ、かつ信号線の組み合わせ以上に変換して揮発性メモリをアクセスすることができる。

【図面の簡単な説明】

【図１】本発明の実施の形態１における秘密情報の解読攻撃対抗方法により秘密情報を揮発性メモリに任意の場所に情報を変換して格納する場合の原理説明図

【図２】本発明における実施の形態１の方法を、揮発性メモリとマイクロプロセッサ間を接続するアドレスバスとデータバスに変換回路を設けることで実現するようにした実施の形態２のブロック図

【図３】本発明の実施の形態２における変換回路を切替スイッチにより構成した場合のブロック図

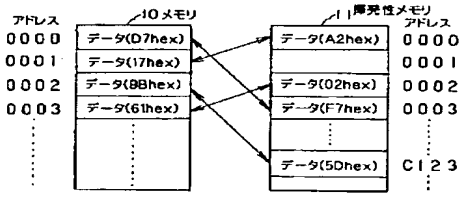
【図４】本発明の実施の形態２における切替スイッチの構成図

【図５】本発明の実施の形態３において変換回路に変換メモリを使用した場合の構成を示すブロック図

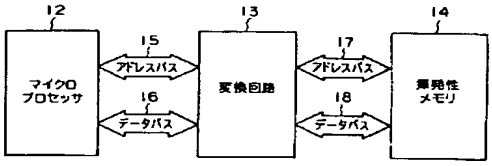
【符号の説明】

１０　変換以前の秘密情報の格納状態を表すメモリ
１１　変換後の秘密情報の格納状態を表す揮発性メモリ
１２　マイクロプロセッサ
１３　変換回路
１４　揮発性メモリ
１５　、１７　アドレスバス
１６、１８　データバス
ＳＷＡ０、ＳＷＡ１　アドレス用切替スイッチ
ＳＷＤ０、ＳＷＤ１　データ用切替スイッチ
１３１　アドレス変換用メモリ
１３２　データ書き込み変換用メモリ
１３３　データ読み込み変換用メモリ
１３４、１３５　データバス切替器

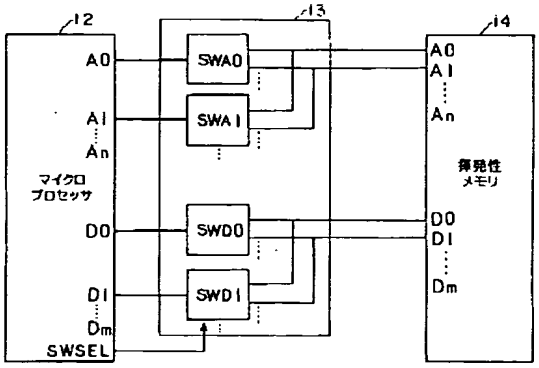
【図１】



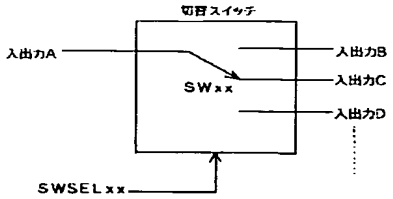
【図２】



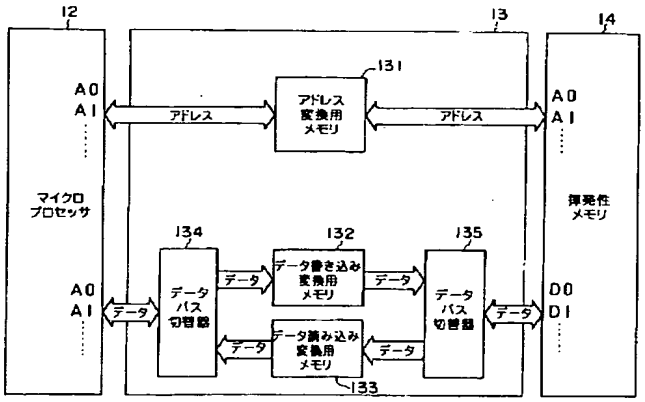
【図３】


12
13
14
A0
A1
An
マイクロプロセッサ
D0
D1
Dm
SWSEL
SWA0
SWA1
SWD0
SWD1
A0
A1
An
揮発性メモリ
D0
D1
Dm

【図４】


切替スイッチ
入出力A
入出力B
入出力C
入出力D
SWxx
SWSELxx

【図５】


12
13
14
131
A0
A1
アドレス
アドレス変換用メモリ
アドレス
A0
A1
マイクロプロセッサ
揮発性メモリ
134
132
135
A0
A1
データ
データバス切替器
データ
データ書き込み変換用メモリ
データ
データバス切替器
D0
D1
データ
データ
データ読み込み変換用メモリ
データ
133